
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	Hon. Madeline Cox Arleo
	:	
v.	:	
	:	
	:	Mag. No. 13-8354
	:	
SEAN ROBERSON and	:	
HUGO REBAZA	:	CRIMINAL COMPLAINT

I, Anthony Gonzalez, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Postal Inspector, United States Postal Inspection Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.




Anthony Gonzalez, Postal Inspector
United States Postal Inspection Service

Sworn to before me, and
subscribed in my presence

December 3, 2013 at
Newark, New Jersey

HONORABLE MADELINE COX ARLEO
UNITED STATES MAGISTRATE JUDGE


Signature of Judicial Officer

ATTACHMENT A

Count One

(Conspiracy to Commit Fraud by Wire, Radio, or Television)

From at least as early as in or around April 2012 through in or around May 2013, in the District of New Jersey and elsewhere, defendants

**SEAN ROBERSON and
HUGO REBAZA**

knowingly and intentionally conspired and agreed with each other and with others to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communications in interstate commerce, certain writings, signs, signals, pictures, and sounds for the purpose of executing such scheme or artifice in a manner affecting a financial institution, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Anthony Gonzalez, a Postal Inspector with the United State Postal Inspection Service (“USPIS”), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

Background

1. At all times relevant to this Complaint, unless otherwise indicated:
 - a. “Embossing” is the act of printing certain information on credit and debit cards. Embossed print appears as the raised print typically appearing on the face of legitimate debit and credit cards and displaying information associated with a particular card, such as the name of the account holder, the account number for the account, and expiration date for the card.
 - b. “CVV” stands for “Card Verification Value” and “CID” stands for “Card Identifier” or “Card Identification Number.” Both are 3- to 4- digit codes embossed on the front or back of legitimate payment cards. Online merchants often require customers to enter a card’s CVV or CID code along with other payment card information prior to entering into online transactions. The purpose of requiring the entry of these codes is to provide some proof that the user of the payment card account information has physical possession of the card.
 - c. “IP address” refers to an Internet Protocol address. An IP address is a unique number assigned to an internet connection. This number is used to route information between devices. Two computers or devices must know each other’s IP addresses to exchange even the smallest amount of information. Accordingly, when one computer requests information from a second computer, the requesting computer specifies its own IP address so that the responding computer knows where to send its response.
 - d. “Proxy services” are services that allow individuals to masquerade their true IP address when accessing the Internet.
 - e. “BitCoin” is a cryptographic-based digital currency, which can be used to pay for goods or services over the Internet, and can be exchanged into United States currency through the use of Bitcoin exchangers.
 - f. Defendant SEAN ROBERSON was a resident of Palm Bay, Florida. ROBERSON was convicted in 2006, in the District of New Jersey, for fraud and related activity in connection with means of identification, in violation of Title 18, United States

Code, Section 1028, for attempting to sell counterfeit driver's licenses and health insurance cards over the Internet.

g. Defendant HUGO REBAZA was a resident of Palm Bay, Florida.

The Investigation

2. The USPIIS and the Federal Bureau of Investigation (“FBI”) have been investigating a seller of (i) authentication features for false identification documents, specifically holographic overlays used on various state-issued driver’s licenses (“Holographic Overlays”), and (ii) customized counterfeit credit and debit cards (“Counterfeit Payment Cards”). The investigation revealed that ROBERSON, REBAZA, and others (collectively, the “Co-Conspirators”), received orders for Holographic Overlays and Counterfeit Payment Cards by, *inter alia*, email.

3. SEAN ROBERSON used an email account, referred to herein as the “Roberson Email Account,” to send and receive orders for such contraband.

4. HUGO REBAZA worked for ROBERSON and was responsible for creating and accessing mailboxes, opened with commercial mail receiving agents (“CMRAs”), which were used, *inter alia*, to receive payment from the Co-Conspirators’ customers.

A. SEAN ROBERSON

The Roberson Email Account

5. On or about May 22, 2013, law enforcement obtained a search warrant in the District of New Jersey, Mag. No. 13-3621, to search the Roberson Email Account. As further detailed below, ROBERSON was identified as the user of the Roberson Email Account.

6. Review of the Roberson Email Account revealed that it was in fact used, from in or around April 2012 through in or around May 2013, to receive and transmit orders for Holographic Overlays and Counterfeit Payment Cards. Review of the Roberson Email Account revealed well over 500 orders for Holographic Overlays and Counterfeit Payment Cards. Review of the Roberson Email Account also revealed that a number of these orders were for delivery to locations within the District of New Jersey.

7. For example, in an email dated May 22, 2013 sent to the Roberson Email Account, ROBERSON received an order for 29 Counterfeit Payment Cards. This email specified the address that the cards were to be sent to, as well as the account number, expiration date, name, and CVV code to appear on each card. Law enforcement has confirmed with the issuing banks that a number of these accounts have since been associated with fraudulent transactions. Based on my training and experience, there is probable cause to believe that the order was for the creation of 29 Counterfeit Payment Cards to be embossed and ultimately encoded with the information provided in the email, which were then used by the individual or individuals placing the order to make unauthorized and fraudulent purchases with the cards.

8. As another example, in an email dated on or about April 10, 2012, ROBERSON sent an email from the Roberson Email Account to one of the Co-Conspirators. The email contained information regarding orders from various individuals for, *inter alia*, the following:

- a. "Barclays blue Visa 2pcs HSBC platnum visa 2pcs Citi thank you MC 2pcs Citi shell MC 2pcs Citi Platinumb – Select 1psc."
- b. "33 embossed (No airline cards like AAdvantage or Alaska.)"
- c. "4 Florida overlays 4 Illinois overlays 4 Maryland overlays 4 New Jersey overlays 4 Pennsylvania overlays 4 Rhode Island overlays 4 South Carolina overlays 4 Wisconsin overlays."

9. Based on my training and experience, as well as the context of the email and review of the Roberson Email Account, the April 10, 2012 email contained multiple orders for Counterfeit Payment Cards and Holographic Overlays.

10. Review of the Roberson Email Account also revealed that at various times, ROBERSON accepted payment by cash, and through virtual currencies such as BitCoin.

ROBERSON is the User of the Roberson Email Account

11. The investigation revealed that the user of the Roberson Email Account frequently used proxy services to masquerade the user's true IP address. However, law enforcement identified a number of emails in the Roberson Email Account indicating the user's true IP address. Law enforcement then compared this IP address to IP addresses used by ROBERSON to conduct online transactions under his real name. On several occasions, the same IP address used by ROBERSON was also used by the user of the Roberson Email Account.

12. For example, the Roberson Email Account contained a number of emails from Mt. Gox, a widely used BitCoin exchanger. These emails indicated that the user of the Roberson Email Account has an account with Mt. Gox. On or about August 27, 2012, the Roberson Email Account received two withdrawal confirmation emails from Mt. Gox indicating that certain withdrawals were made from the IP address 97.104.141.223 (the "Roberson IP Address"). Law enforcement determined that the Roberson IP Address is owned by the internet service provider Bright House Networks Information Services ("BHNIS"), and not a proxy service. On or about July 17, 2013, in response to a federal grand jury subpoena, BHNIS informed law enforcement that it provides internet service to ROBERSON's home.

13. BHNIS indicated that its records only went back to September 14, 2012, and did not go back far enough to determine which of its subscribers was assigned the Roberson IP Address on August 27, 2012, the date of the Mt. Gox withdrawals from the Roberson IP Address.

14. However, through additional investigation, law enforcement discovered an account with the online retailer, Amazon.com, held by SEAN ROBERSON (the "Roberson Amazon Account"). Law enforcement subpoenaed Amazon for, *inter alia*, IP addresses used by ROBERSON to purchase goods online from Amazon. On or about September 23, 2013, in response to a federal grand jury subpoena, Amazon confirmed that the Roberson Amazon Account was accessed approximately 6 times between June 4, 2012 and July 24, 2012, from the

Roberson IP Address to make purchases. Amazon also confirmed that certain purchases made on or after September 14, 2012, were made from IP addresses assigned to ROBERSON's office location, as confirmed by BHNIS. Amazon additionally confirmed that the Roberson Amazon Account was also accessed approximately 11 times between March 7, 2013 and July 8, 2013, from IP addresses assigned by BHNIS to ROBERSON's office at the dates and times of access to the Roberson Amazon Account.

15. In sum, the same IP address used by ROBERSON on or about July 24, 2012 to purchase items from Amazon was used by the user of the Roberson Email Account on or about August 27, 2012 to make withdrawals from Mt. Gox.

16. Additionally, many of the purchases made through the Roberson Amazon Account were for items commonly used to make fake identification cards and counterfeit credit cards. Moreover, as detailed below, some of the items purchased through the Roberson Amazon Account are referenced in the Roberson Email Account.

17. For instance, on or about August 3, 2011, ROBERSON ordered a total of 2,000 white PVC cards with magnetic stripes through the Roberson Amazon Account. Based on my training and experience, these are the types of cards used to create Counterfeit Payment Cards.

18. Additionally, on or about August 25, 2011, ROBERSON ordered 4 rolls of " Fargo 84061 YMCFK Full-Color Ribbon for HDP5000 ID Card Printer" through the Roberson Amazon Account. Based on my training and experience, the HDP5000 ID Card Printer is a high-end printer capable of printing fake identification cards and Counterfeit Payment Cards.

19. Review of the Roberson Email Account revealed two emails, dated June 7, 2012 and November 29, 2012, indicating that the user of that account uses "YMCFK" film. Additionally, in an April 12, 2012 email sent from the Roberson Email Account to a company that provides software used to print and encode cards, ROBERSON indicated that, "[c]urrently we are using 2 HDP5000 printers."

Undercover Purchases

20. On or about July 24, 2013, an undercover FBI agent (the "UC") placed an order for Holographic Overlays and Counterfeit Payment Cards from ROBERSON. On or about July 30, 2013, the UC received, by mail, a package from an address in Melbourne, Florida. Inspection of the contents of that package confirmed that it contained the Holographic Overlays and Counterfeit Payment Cards ordered by the UC.

21. On or about October 2, 2013, the UC ordered additional Counterfeit Payment Cards from ROBERSON. On or about October 9, 2013, the UC again received, by mail, a package from an address in Melbourne, Florida, containing the Counterfeit Payment Cards ordered by the UC.

B. HUGO REBAZA

22. As further described below, REBAZA was responsible for picking up packages of contraband and criminal proceeds delivered to the Co-Conspirators at one or more CMRAs.

23. Review of the Roberson Email Account revealed that the Co-Conspirators used a number of CMRAs to receive payment for Holographic Overlays and Counterfeit Payment Cards, and to receive orders of Holographic Overlays from individuals overseas, to resell to their customers.

- a. For example, in a May 2, 2013 email from the Roberson Email Account to another email address associated with a Co-Conspirator in China ("CC-1"), ROBERSON requested a total of "20,000 hologram overlays" for the following ten states: Delaware; Florida; Ohio; Connecticut; Illinois; Kentucky; Maryland; Mississippi; New Jersey; and South Carolina. In response, CC-1 quotes a price of "6100USD." Based on my training and experience, as well as the context of the communication, there is probable cause to believe that ROBERSON was referring to the purchase of Holographic Overlays from CC-1.
- b. Subsequently, in a May 8, 2013 email from the Roberson Email Account to CC-1, ROBERSON indicated that payment for the Holographic Overlays would be sent in three separate wires to locations overseas, and asked that the holograms be sent to a name, referred to herein as "DropName-1," at an address for a CMRA in West Melbourne, Florida.

24. Review of the Roberson Email Account also revealed that the Co-Conspirators used CMRAs to receive payment for orders of Holographic Overlays and/or Counterfeit Payment Cards.

- a. For example, in a January 2013 email exchange between ROBERSON, using the Roberson Email Account, and another Co-Conspirator ("CC-2"), CC-2 referred to various orders CC-2 placed with ROBERSON for Counterfeit Payment Cards. At the end of the exchange, in an email dated January 29, 2013, ROBERSON indicated that he would be filling some of CC-2's orders for Counterfeit Payment Cards, and added "[a]lso worker got ID today so hopefully tonight will get the box open." In a follow up e-mail sent later that same day, ROBERSON provided the name, DropName-1, and an address for a CMRA in Indialantic, Florida (the "Indialantic CMRA").

25. Law enforcement confirmed that the address provided for the Indialantic CMRA is indeed the address for a mailbox at a CMRA called "Atlantic Pack & Parcel." In response to a USPS inquiry, Atlantic Pack & Parcel confirmed that the Indialantic CMRA mailbox address referenced in the email above was opened by an individual under the name, DropName-1, and provided copies of the account-opening documents, including copies of the identification provided by the individual who opened the account.

26. The records relating to the Indialantic CMRA mailbox account revealed that the account was opened on or about January 29, 2013, as indicated in ROBERSON's email described above.

27. Law enforcement's review of the identification card used to open the Indialantic CMRA mailbox account revealed that it was a fake New Jersey driver's license in the name of DropName-1. Comparison of the image on the fake driver's license, surveillance video from Atlantic Pack & Parcel showing the individual picking up parcels from the Indialantic CMRA mailbox, and DMV records, revealed that the individual pictured in the fake identification and seen on the surveillance video accessing the Indialantic CMRA mailbox is REBAZA.

28. Additionally, on or about July 26, 2013, the owner of Atlantic Pack & Parcel advised law enforcement that the individual who rented the Indialantic CMRA mailbox came in to Atlantic Pack & Parcel and picked up a Federal Express parcel that was mailed to the Indialantic CMRA mailbox. The owner advised that the individual was driving a Tan Dodge Durango and provided the license plate number for the vehicle. Florida DMV records revealed that the vehicle was registered to REBAZA.